

U.S. Department of Homeland Security

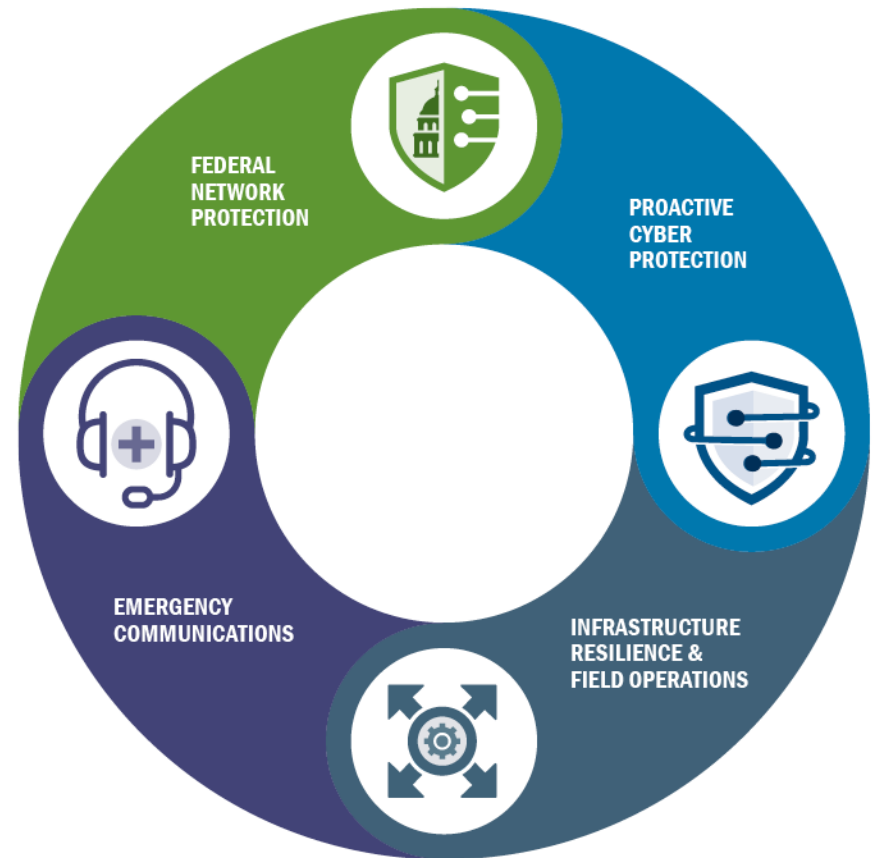
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY



CISA
CYBER+INFRASTRUCTURE

The Nation's Risk Managers

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure



Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.



FEDERAL NETWORK
PROTECTION



PROACTIVE CYBER
PROTECTION



INFRASTRUCTURE
RESILIENCE &
FIELD OPERATIONS



EMERGENCY
COMMUNICATIONS

Presidential Policy Directive 41 – Concurrent Lines of Effort

- **Threat Response**
 - Threat response activities include conducting appropriate law enforcement and national security investigative activities; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.
- **Asset Response**
 - Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.
- **Intelligence Support**
 - Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.



ALABAMA PROBATE JUDGES SUMMER CONFERENCE

- Protective Security Advisors (PSA)
 - North and South Districts
- PSA Visits
 - Resources briefing
 - Protected Critical Infrastructure Information (PCII)
 - Training
 - Information Sharing and Outreach
- Security Walk-through
 - What is entails
 - Up to 2 facilities in each county
- Written Report
 - Issues
 - Options for Consideration

ALABAMA PROBATE JUDGES SUMMER CONFERENCE

North Alabama PSA Greg
Carden

Gregory.carden@hq.dhs.gov
202-841-1907

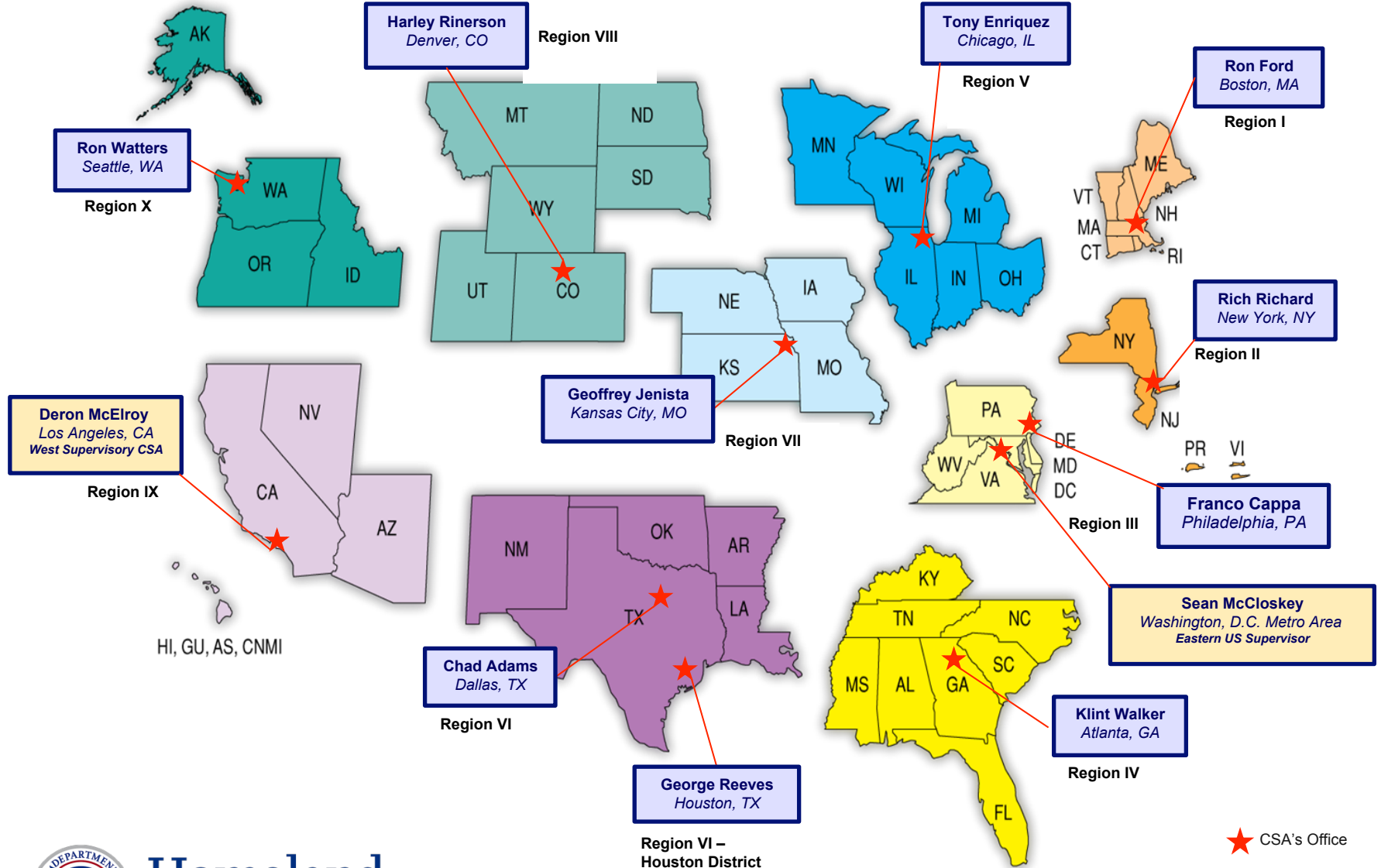
Please contact Greg or I to set up a PSA
Visit and Security Walk-through of your
facilities.

South Alabama PSA
Kirk Toth

Kirk.toth@hq.dhs.gov
850-621-3264



Cybersecurity Advisor (CSA) Locations



**Homeland
Security**

CSA Program Mission

To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Territorial, and Tribal (SLTT) governments.

Cyber Security Advisor (CSA) Program in recognition that a regional and national focused cyber security presence is essential to protect critical infrastructure.

CSAs represent a front line approach and promote resilience of key cyber infrastructures throughout the U.S. and its territories.



CSA Program Activities

CSAs support four key DHS goals:

Cyber Preparedness

Risk Mitigation

Incident & Information Coordination

Cyber Policy Promotion & Situational Awareness

CSAs facilitate three assessments:

Cyber Resilience Reviews (CRR)

















Cyber Infrastructure Surveys (C-IST)

External Dependency Reviews (EDM)

CSAs participate in local / regional cyber working groups, mostly organized by Federal and state partners



16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

 CHEMICAL	DHS (CISA)	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	DHS (CISA)	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	DHS (CISA)	 GOVERNMENT FACILITIES	GSA & DHS (FPS)
 CRITICAL MANUFACTURING	DHS (CISA)	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	DHS (CISA)	 INFORMATION TECHNOLOGY	DHS (CISA)
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
 EMERGENCY SERVICES	DHS (CISA)	 TRANSPORTATIONS SYSTEMS	(TSA & USCG)
 ENERGY	DOE	 WATER	EPA

Today's Risk Landscape

America remains at risk
from a variety of threats:



ACTS OF TERRORISM



CYBER ATTACKS



EXTREME WEATHER



PANDEMICS



ACCIDENTS
OR TECHNICAL
FAILURES

Cyberspace: Foundational to Our World

- Automation, technology, and network communications have become increasingly essential to our daily lives.
- The amount of information and data stored electronically has grown.
- There is a vast interconnectedness of relationships and dependencies, for example
 - government – private sector – international
 - third-party vendors
 - linkages within organizations
- As a result, the country is dependent on the cyber resilience of its critical infrastructure, such as, the power grid, banking and financial systems, and telecommunications



**Homeland
Security**

A Growing Challenge

- **Scale:** The number of cyber attacks has never been greater.
- **Sophistication :** Cyber attacks are increasing in complexity.
- **Trends:** Attackers are increasing their advantage.
- **Attack Surface:** Growing volumes of data = more targets.



Homeland
Security

Threat Landscape

(U//FOUO) Threat to Critical Infrastructure Facilities, Networks and Sensitive Information

Damage to
Critical Infrastructure

Disruption to Critical Infrastructure

Theft of Intellectual Property

Theft of Sensitive Financial Transaction Data

Theft of Sensitive Information (PII)

Distributed Denial of Service (DDOS)

Web Defacement

State Actors with
Greater Capabilities

State Actors with
Lesser Capabilities

Cybercriminals

Criminal Hackers






Terrorists






NOTE: Insider assistance may amplify the likelihood and impact of a Cyber Attack.



Homeland
Security

IT vs. OT

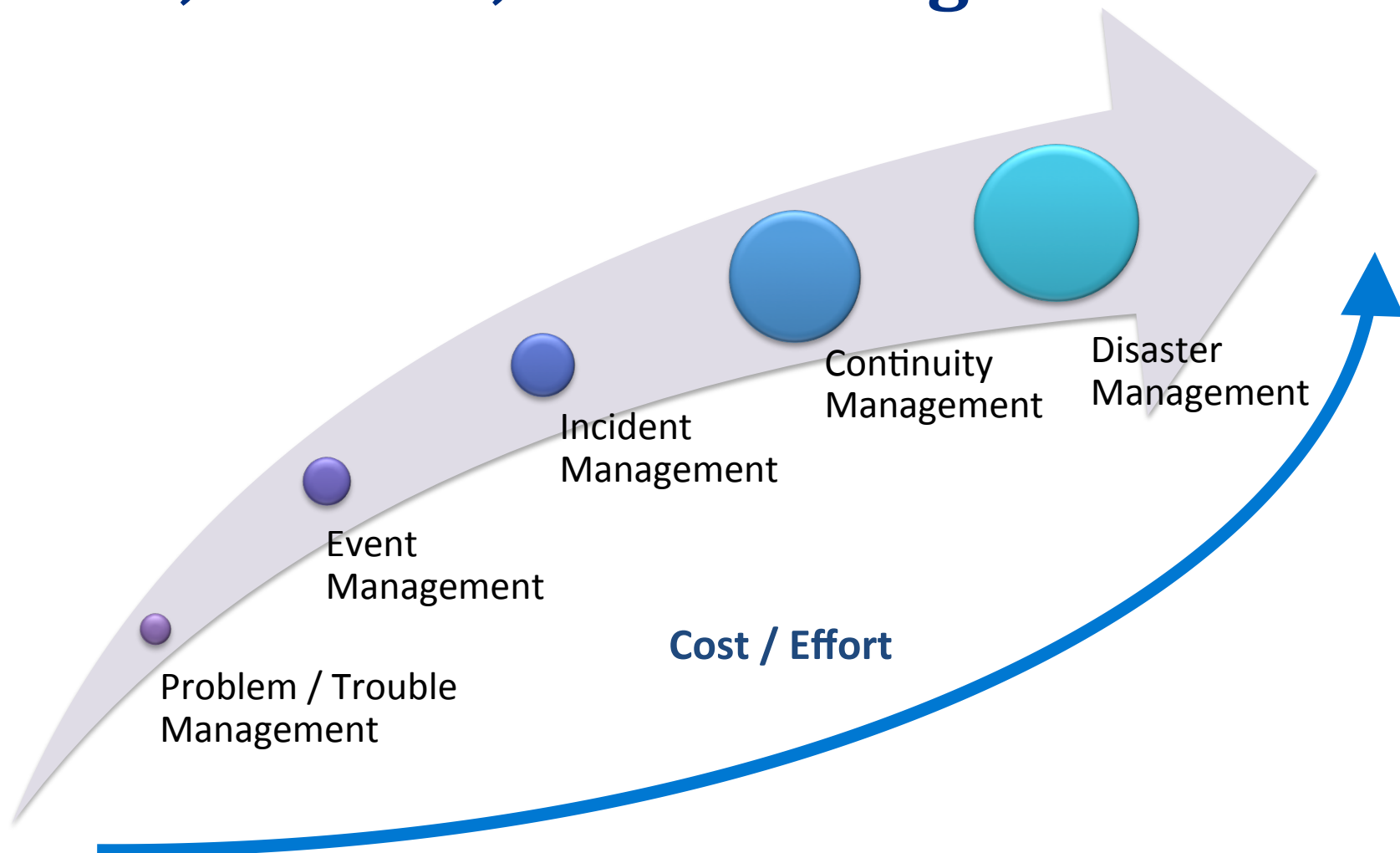
SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
 ANTIVIRUS & MOBILE CODE COUNTER-MEASURES	Common & widely used	Can be difficult to deploy
 SUPPORT TECHNOLOGY LIFETIME	3 to 5 years	Up to 40+ years
 OUTSOURCING	Common/widely used	Rarely used (vendor only)
 APPLICATION OF PATCHES	Regular/scheduled	Slow (vendor specific, compliance testing required)
 CHANGE MANAGEMENT	Regular/scheduled	Legacy based – unsuitable for modern security

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
 TIME CRITICAL CONTENT	Delays are usually accepted	Critical due to safety
 AVAILABILITY	Delays are usually accepted	24 x 7 x 365 x forever (Integrity also critical)
 SECURITY AWARENESS	Good in both private and public sector	Generally poor inside the control zone
 SECURITY TESTING/AUDIT	Scheduled and mandated	Occasional testing for outages / audit for event recreation
 PHYSICAL SECURITY	Secure	Traditionally good

How Are **You** Targeted by Foreign Intel?



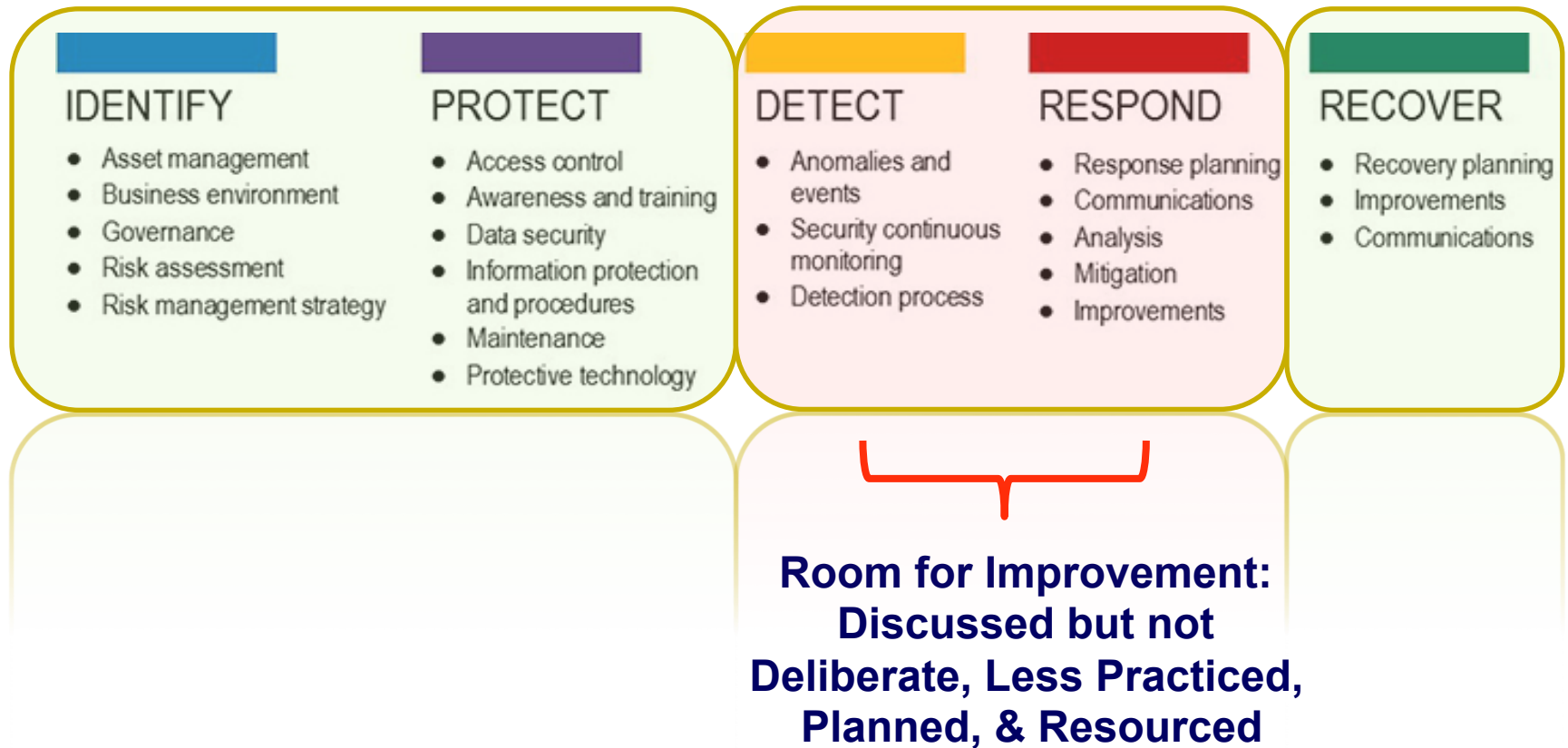
Operational Planning for Cyber Security Events, Attacks, and Contingencies



**Homeland
Security**

CSF and the State of Cybersecurity Management

Status Quo: Practiced, Planned, & Resourced



**Homeland
Security**

A Wide Range of Offerings for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
 - US-CERT Operations Center
 - **Remote / On-Site Assistance**
 - **Malware Analysis**
 - **Incident Response Teams**
 - ICS-CERT Operations Center
 - **ICS-CERT Malware Lab**
 - **Incident Response Teams**
 - Cyber Exercise Program
- Cyber Security Advisors
- Protective Security Advisors
- Preparedness Activities
 - **National Cyber Awareness System**
 - **Vulnerability Notes Database**
 - **Security Publications**
 - **Technical Threat Indicators**
 - **Cybersecurity Training**
 - **Information Products and Recommended Practices**
- Control Systems Evaluations
 - **Cyber Security Evaluation Tool**
 - **ICS Design Architecture Reviews / Network Architecture Analysis**
- Other Cyber Security Evaluations
 - **Cyber Resilience Review**
 - **Cyber Infrastructure Survey**
 - **Cyber Hygiene service**
 - **Risk and Vulnerability Assessment (aka “Pen” Test)**



**Homeland
Security**



Contact Information

Evaluation Inquiries

cyberadvisor@hq.dhs.gov

General Inquiries

cyberadvisor@hq.dhs.gov

DHS Contact Information

Sean McCloskey

Program Director, Cyber Security
Advisor Program

Sean.mccloskey@hq.dhs.gov

Klint Walker

Cyber Security Advisor, Region IV

Klint.walker@hq.dhs.gov

+1 404-895.1127

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications



MS-ISAC®

Multi-State Information
Sharing & Analysis Center®



**Elections
Infrastructure
ISAC**

Elections Security in a Connected World:

Your Guide to the Elections Infrastructure ISAC

Kateri Gill

June 10, 2019

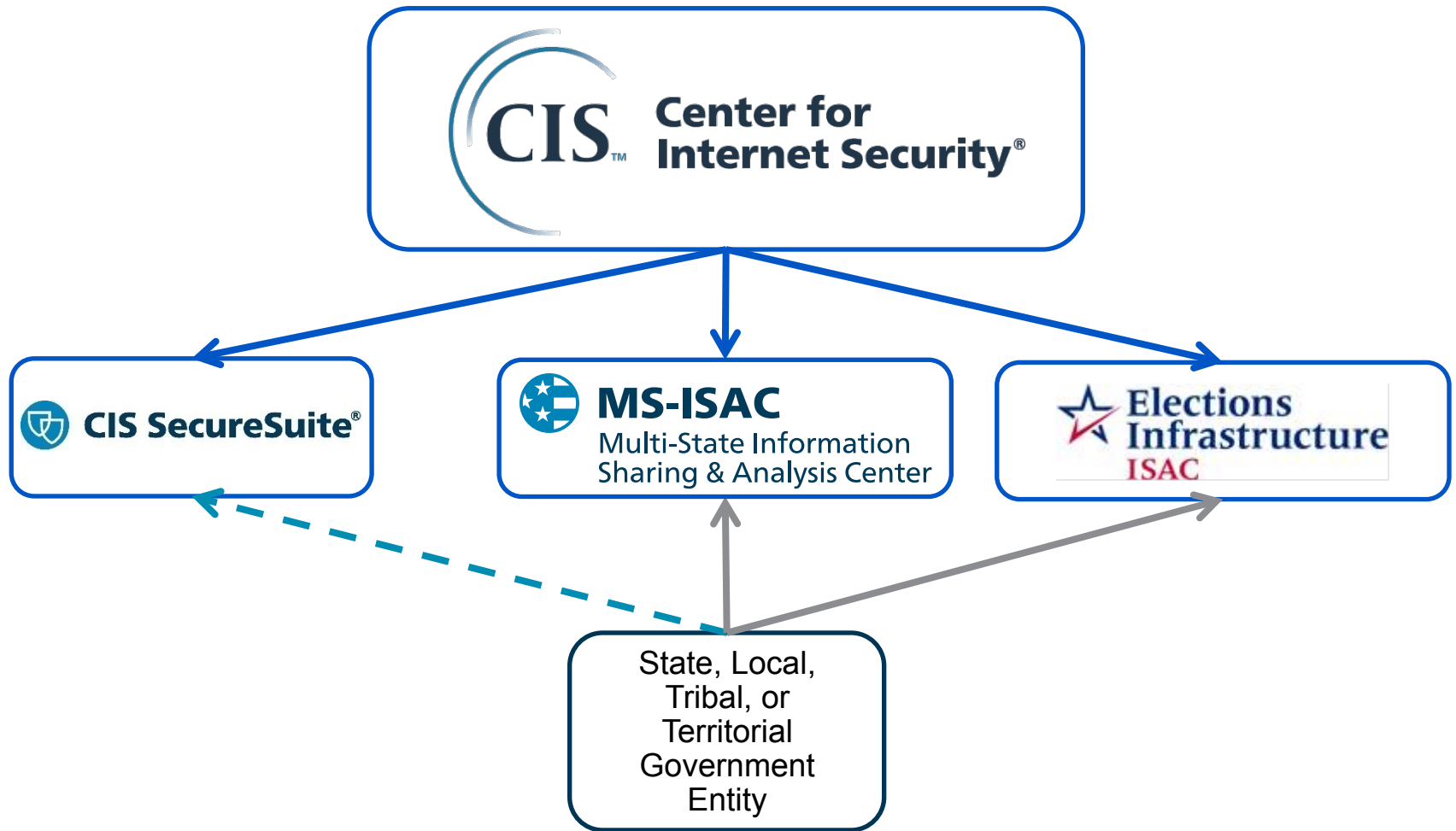


MS-ISAC

Multi-State Information
Sharing & Analysis Center



**Elections
Infrastructure**
ISAC





How We Got Here

Summer
2016

- Public reporting of voter registration compromises

July
2017

- Election Critical Infrastructure Working Group meets at MS-ISAC HQ

October
2017-
February
2018

- MS-ISAC Pilot for Elections (NJ, VA, IN, TX, CO, UT, WA)

March
2018

- EI-ISAC Official Launch

January
2017

- Intelligence Community Assessment
- Critical Infrastructure Designation

September
2017

- Election Infrastructure Subsector Government Coordinating Council (EIS-GCC) established
- MS-ISAC Pilot for Elections Approved

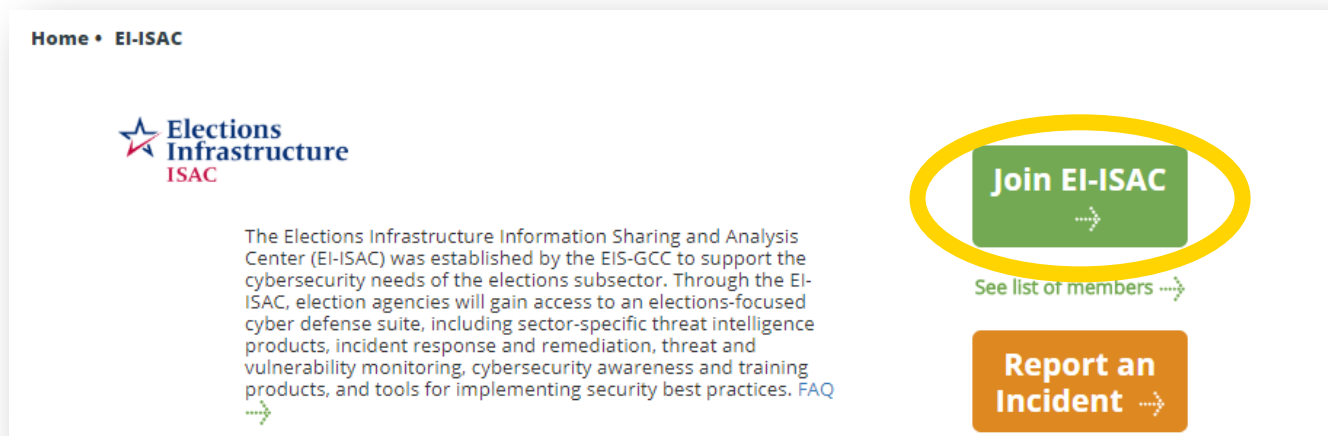
February
2018

- EIS-GCC votes to establish EI-ISAC



About EI-ISAC Membership

Free and Voluntary
No Mandated Information Sharing
Registration is the only requirement!



To join or get more information:
<https://learn.cisecurity.org/ei-isac-registration>



Membership and Albert Overview (as of 5/30)

Membership



50 State Election Offices



1600 Local Election Offices (48 states)



4 Territorial Election Offices



7 Election Official Associations



15 Election Vendors

49 State Election Sensors

23 Bottom-Up Local Election Sensors

71 State-Funded Local Election Sensors

2 Territorial Election Sensors



Albert
Sensor
Coverage



Alabama Membership

Alabama Office of the Secretary of State

Mobile County Probate Court

St. Clair County Probate Court

St. Clair County Circuit Clerk



An Elections-focused Cyber Defense Suite

- 24x7x365 network monitoring
- Incident response and forensics
- Threat and vulnerability monitoring
- Election-specific threat intelligence
- Training sessions and webinars
- Promote security best practices



www.cisecurity.org/ei-isac



24 x 7 Security Operations Center

Central location to report any cybersecurity incident

- **Support:**
 - Network Monitoring Services
 - Research and Analysis
- **Analysis and Monitoring:**
 - Threats
 - Vulnerabilities
 - Attacks
- **Reporting:**
 - Cyber Alerts & Advisories
 - Web Defacements
 - Account Compromises
 - Hacktivist Notifications



To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org



Perception Management



TLP: WHITE



What Could Possibly Happen?

Florida Man Admits Killing Goat and Drinking Its Blood For Pagan Sacrifice, Would Still Like to be Senator gq.com/story/augustus...

5:52 PM - Oct 5, 2015



Yes, This Libertarian Senate Candidate Really Did Sacrifice
Everything you need to know about Augustus Sol Invictus
gq.com



Attack During

, 2018 11:42 AM 1



Florida Man
@_FloridaMan



Florida Man Arrested For Beating Drag Queen With Tiki Torch While Dressed as Member of KKK, Now Running For Mayor |

blogs.browardpalmbeach.com/pulp/2014/10/d...

10:03 PM - Oct 23, 2014

♡ 678 💬 1,154 people are talking about this



Computer Emergency Response Team

- Incident Response (includes on-site assistance)
- Network & Web Application Vulnerability Assessments
- Malware Analysis
- Computer & Network Forensics
- Log Analysis
- Statistical Data Analysis
- Penetration Testing

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org



Understanding the News

Data Breach or Hoax?

Voter Records for Sale on RAID Forums

October 5, 2018

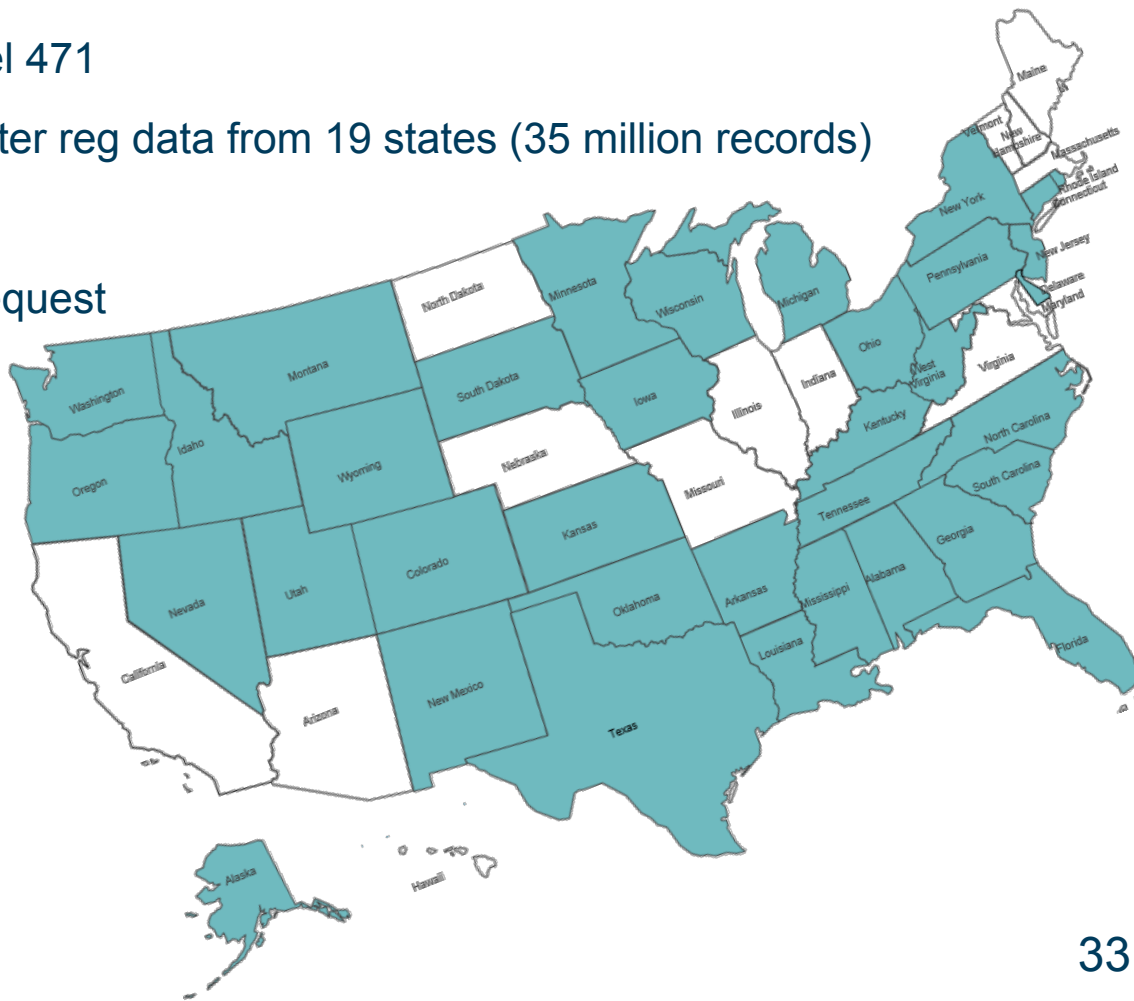
- Identified by Anomali Labs and Intel 471
- Malicious Actor “Downloading” - voter reg data from 19 states (35 million records)
- Pricing: \$150-\$12,500
- Information typically available by request

October 17, 2018

- “Backdoor” claim
- Updated data on a weekly basis

October 20, 2018

- All 50 voter registration databases
 - 200 million voter records
 - \$61,000





Elections Weekly News Alert

- **EI-ISAC analysis to provide key context**
 - General election industry or election security reports
 - Legislative action on election security issues
 - Best practice examples from peers in the election community
 - General technology/cybersecurity stories that may have an election link/impact
- **Released on Wednesday afternoons**

TLP: WHITE
EI-ISAC Weekly News Alert

TO: All EI-ISAC Members and Partners

DATE: March 28, 2018

SUBJECT: EI-ISAC Weekly News Alert 3/28/2018

The EI-ISAC Weekly News Alert is a summary of open-source reporting on election security and topics that may be of interest to elections officials. The Weekly News Alert is intended to provide situational awareness of the cyber risk landscape and cybersecurity best practices to election officials through open source news reporting and analysis by the EI-ISAC and other experts. If you would like to submit security-related stories that may be of interest to the elections community, please contact elections@cisecurity.org.

U.S. Consolidated Appropriations Act of 2018 Grants \$380 Million for Election Security – [Reuters](#) (3/21/18)

TLP: WHITE On March 23, 2018, President Trump signed into law the \$1.3 trillion [Consolidated Appropriations Act of 2018](#). The Act appropriates the outstanding \$380 million from the Help America Vote Act ([HAVA](#)) for the purposes of improving election security. The Election Assistance Commission (EAC) will distribute funds within 45 days, with a minimum funding threshold of \$3 million per state and \$600,000 per territory. States must agree to match 5% of grant funds within two years. Separately included in the Act is a mandate for several federal entities to launch a comprehensive supply chain review prior to the acquisition of new technology and/or associated equipment.

***EI-ISAC Analyst Note:** Though the supply chain provision does not affect state or local election offices, it further highlights the wider community's focus on addressing potential supply chain and procurement security risks. The CIS [Handbook for Election Infrastructure Security](#) includes an appendix addressing security in supplier relationships and the EAC provides [example procurement resources](#) from multiple states.*

TLP: WHITE



Cybersecurity Spotlight

- **Key Security Terms and Best Practices**
 - What it is
 - Why does it matter
 - What you can do
- **Released on Friday afternoons**

TLP: WHITE



Encryption

What it is: Encryption is the process whereby data is converted from a readable form (i.e., plaintext), to an encoded form (i.e., ciphertext). This encoding is designed to be unintelligible except by parties that possess a key to reverse the encoding process. This reversal process is called decryption. Data is encrypted using a mathematical algorithm that relies on passcodes (keys) that are typically randomly generated. The most trusted encryption algorithms are considered secure because they have been publicly available for years and have not been broken. An attack on data encrypted with a trusted encryption algorithm could take years for even the most powerful computers to break.

There are two types of encryption: asymmetric (public key) encryption and symmetric (private key) encryption.

	Asymmetric	Symmetric
Keys	2 keys – public (to be shared) and private (secret and possessed by only 1 person)	1 key – private (secret but shared between two or more partners)
Process	The sender encrypts information with recipient's public key and the recipient decrypts information with their private key	The sender encrypts information with a private key and the recipient decrypts information with the same private key
Speed	Slower	Faster

An easy way to understand these two types of encryption is two different types of lockboxes. In symmetric cryptography, you have a lockbox with one slot for a key. You make two copies of the key, and you give one to your friend. You lock the box with your copy, and when your friend comes along, they use their copy of the same key to unlock it.

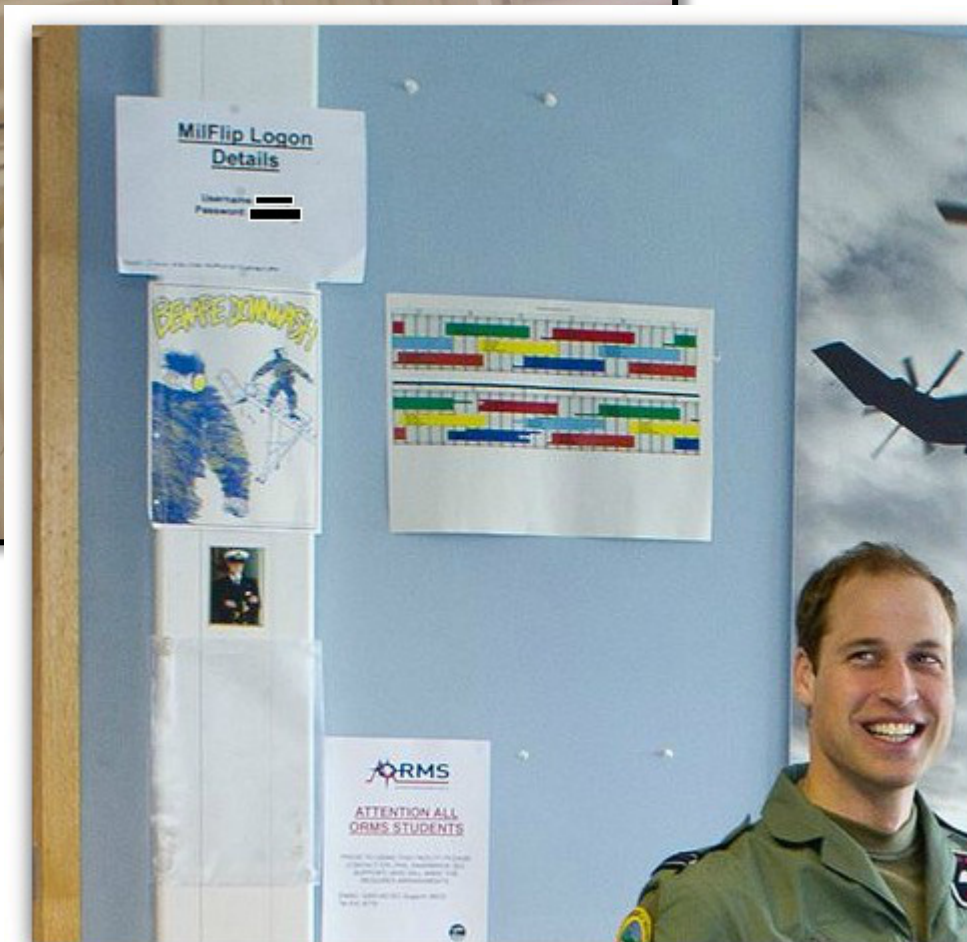
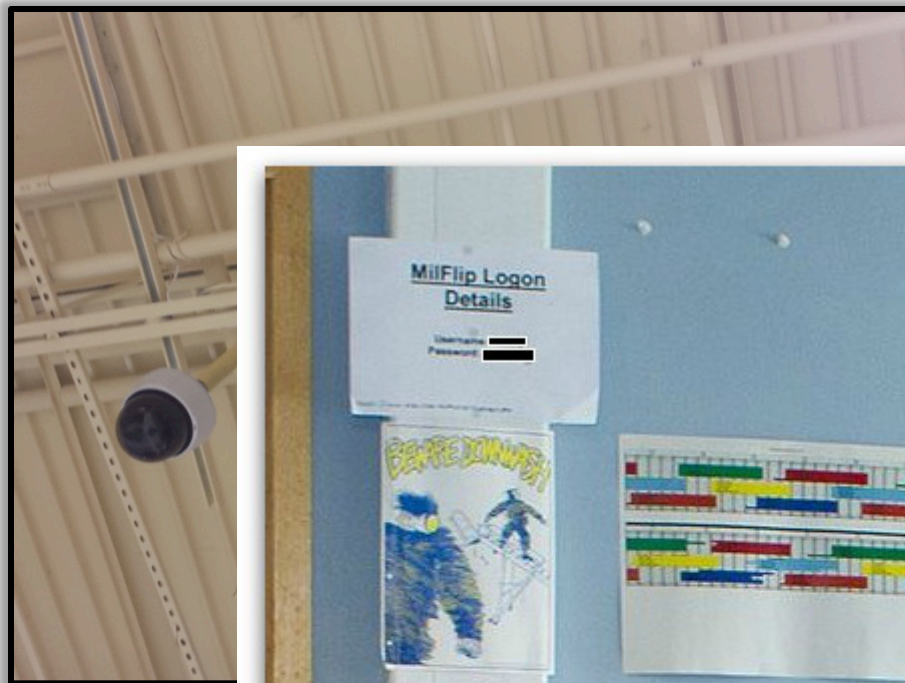
Asymmetric cryptography is different. It's more like a deposit dropbox at a bank. The bank publishes the location of the dropbox (the public key), and once you drop your deposit into it, it's secure until the bank opens the box with the one and only copy of their key (the private key). Anyone can make a deposit once they know the location of the box, but only the bank can get deposits out.

Why does it matter: Encryption allows for the confidential storage and transmission of data, as well as proof that it originated with the person who claims to have sent it. Encrypting personally identifiable information (PII) with good encryption algorithms protects the data from accidental disclosure in the case of a data breach or malware infection. Elections offices may maintain a number of systems that utilize encryption and are responsible for identifying data that should be encrypted. This may

TLP: WHITE



Employee Mistakes



TLP: WHITE



Election-specific Cyber Alerts

- **Short e-mail alerts regarding immediate threats**
 - Targeted at both executive and technical staff
- **Provides overview of activity and actionable recommendations**
 - Executive Overview
 - Executive Recommendations
 - Technical Overview
 - Technical Recommendations

TLP: **AMBER**

MS-ISAC ELECTIONS PILOT CYBER ALERT

TO: MS-ISAC Elections Pilot Participants



Malicious Code Analysis Platform

A web based service that enables members to submit and analyze suspicious files in a controlled and non-public fashion

- Executables
- DLLs
- Documents
- Quarantine files
- Archives
- URLs

Or just forward suspicious emails to
submission@malware.cisecurity.org

Ukraine's Critical Infrastructure - 2015


- Boryspil International Airport – Kiev, Ukraine
- Power Grid Shut Down
- 225,000 customers lost power for 6 hours
- BlackEnergy Malware
- Attributed to Russia





Elections Sector Quarterly Report & Call

- Compiles analysis of elections-specific events identified by/reported to EI-ISAC
- Provides highlights of EI-ISAC activities



TLP: AMBER

EI-ISAC
Quarterly Threat Report
(July 12, 2018 – Q1 & Q2'18)

Table of Contents

By the Numbers.....	1
Incident Analysis	1
Monitoring Analysis	2
Vulnerability Management Program (VMP).....	3
Information Sharing	3
EI-ISAC Products Disseminated (2018).....	4
Other Key Products (2018).....	4
Top News (2018).....	4
EI-ISAC Speaking Engagements (Q3 2018).....	6
EI-ISAC Membership.....	6

By the Numbers

Open Source Notifications: [redacted]
Member Reported Activity: [redacted]
Incident Response [redacted]
Election Alert Sensors: [redacted]
- Actionable Notifications: [redacted]
VMP Notifications: [redacted]
- Vulnerable Web Servers: [redacted]
- Vulnerable Services [redacted]
Election Products Disseminated: [redacted]
EI-ISAC Membership: [redacted]

Incident Analysis

As part of this analysis, the EI-ISAC monitored potentially malicious activity during the 2018 primary elections. Additional activity identified or reported by election offices in the first half of 2018 included suspicious emails, botnets, tech support scams, and a compromised web server.

Spotlight: 2018 Primary Elections Activity

The EI-ISAC, in partnership with the U.S. Department of Homeland Security (DHS), maintained a heightened level of awareness during the 2018 primary season. EI-ISAC members and open sources reported a limited number of events occurring during the Q2 primaries.



- Meeting

Layouts

Pods

Audio

Attendee List (1)

Active Speakers

Hosts (1)

Ben Spier

Presenters (0)

Participants (0)

Contact Information

Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC)
Multi-State Information Sharing & Analysis Center (MS-ISAC)
Security Operations Center
918-266-3488
7x24 SOC 1: 866-787-4722
SOC@security.org

""READ FIRST"" National Cyber Situational Awareness Room - (U//FOUO) TLP: AMBER

11

T

Z

T

Welcome EI-ISAC Members to the National Cyber Situational Awareness Room!

The National Cyber Situational Awareness Room (NCSAR) is being opened to state and local election offices in Colorado, Maryland, Mississippi, New York, Oklahoma, South Carolina, and Utah for the duration of the June 26, 2018 Primary Election. The EI-ISAC operates the National Cyber Situational Awareness Room for EI-ISAC members in jurisdictions holding a primary or general election. Prior to high profile elections, the room may be open several days in advance of or following the election. The room provides a centralized information sharing platform for the elections community and federal partners regarding cybersecurity threats to election infrastructure.

Features of the room include:

 - **Chat:** Most activity occurs here, where state and local election officials can communicate publicly or with a specific user to share information on cybersecurity events in their jurisdiction.
 - **Highlights:** Reported incidents and Other Key Items of Note from the Primary Election will be recorded here by an EI-ISAC staff member. This will also include reported events from previous primaries;
 - **Events Calendar:** Key Upcoming Events Throughout the Day Will Be Posted Here (Please contact EI-ISAC staff if you would like to add an event).
 - **File Share:** The EI-ISAC will post any alerts or products for download throughout the day. The File Share pod currently has products on several common attacks and the EI Security Handbook (Please contact EI-ISAC staff if you would like a file uploaded).

Please be sure that your username appears as: <State> <Elections Office> <Full Name>
Changes can be made under the drop down menu just right of the "Attendee List" toolbar. Select "Edit My Info"

If you do not provide an affiliation or do not meet the criteria for entry, a Host will remove you from the room.

Chat - TLP: AMBER (Everyone)

----- (06/25/2018 08:57) -----
EI-ISAC - Ben Spier: Welcome Everyone to the National Cyber Situational Awareness Room and thanks for joining us! Please feel free to use this room to share information about cyber events ongoing during the course of today's primary with other states or local election offices. If you are experiencing an incident we are happy to assist you through this room or by contacting our 24x7 Security Operations Center at 866-787-4722 or SOC@security.org

Highlights - (U//FOUO) TLP: AMBER

11

T

Z

T

As of 6:00 AM ET:

No incidents or suspicious activity have been reported by EI-ISAC members.

Previously Reported Incidents:

 - May 1 Primary
 - A local election office reported a denial of service attack affecting their election night reporting webpage.
 - May 8, 15, 22 Primaries
 - No incidents or suspicious activity reported
 - June 5 Primary
 - Some counties in three states reported e-Pollbook issues due to administrative errors or connection issues. Affected counties reverted to paper backups or affidavit ballots as appropriate. No malicious activity was identified.
 - June 12, 19 Primaries
 - No incidents or suspicious activity reported

Events Calendar - (U//FOUO) TLP: AMBER

11

T

Z

T

Polls Open
CO - 7:00AM MT
MD - 7:00 AM ET
MS - 7:00 AM CT
NY - 6:00 AM ET
OK - 7:00 AM CT
SC - 7:00 AM ET
UT - 7:00 AM MT

Polls Close
CO - 7:00PM MT
MD - 8:00 PM ET
MS - 7:00 PM CT
NY - 9:00 PM ET
OK - 7:00 PM CT
SC - 7:00 PM ET
UT - 8:00 PM MT

File Share - (U//FOUO) TLP: AMBER

Name	Size
NCSAR - Standard Operating Procedures.pdf	570 KB
Guide to DDoS Attacks.pdf	563 KB
General Security Recommendations.pdf	233 KB
SQL Injection White Paper.pdf	296 KB
Spear Phishing.pdf	240 KB
EI Security Handbook.pdf	1 MB
Cross-Site Scripting_185914579.pdf	232 KB
SQLi Recommendations.pdf	227 KB

Upload File...

Download File(s)



ISAC Annual Meeting

2020 Annual Meeting

Baltimore, MD

Date TBD





Handbook for EI Security

- Intended for Elections Officials and Technical Support Teams
- Analyzes the risks of key election system components
- Describes specific technical controls and processes to improve security
- Assessment tool available



Order Hard Copies:

<https://learn.cisecurity.org/ei-handbook>

<https://www.cisecurity.org/elections-resources>



Where to Start

Best Practice	Best Practice Title	Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
4	Only utilize approved and managed USB devices with appropriate device encryption and device authentication	Devices	Network Connected	High	No	Medium	Low
8	If wireless is required, ensure all wireless traffic use at least Advanced Encryption Standard (AES) encryption with at least Wi-Fi Protected Access 2 (WPA2)	Devices	Network Connected	High	No	Medium	Low
14	Perform system testing prior to elections (prior to any ballot delivery), such as acceptance testing	Process	Network Connected	High	No	Medium	Low
17	Deploy application whitelisting	Software	Network Connected	High	No	Medium	Low
18	Work with election system provider to ensure base system components (e.g., OS, database) are hardened based on established industry standards	Software	Network Connected	High	No	High	Low
55	For data transfers that utilize physical transmission, utilize tamper evident seals on the exterior of the packaging	Devices	Indirectly Connected	High	No	Medium	Low
64	Only use the devices for election related activities	Software	Indirectly Connected	High	No	Medium	Low



Election Security Services Checklist

- Prioritized action items and tools tied to the EI Handbook and CIS Controls
- Descriptions of key cybersecurity tools
- Links to available services from EI-ISAC, DHS, or GSA

Key: CIS Handbook Best Practices CIS Controls What It Is Where to get It

Monitor Your Network

7 & 42 12

Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. Network monitoring should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based intrusion detection and intrusion prevention systems (IDS and IPS). It is also critical to filter both inbound and outbound traffic.

[EI-ISAC, GSA Schedule 70 132-44 CDM Tools](#)



The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) is a voluntary and collaborative effort based



DHS Continuous Diagnostics and Mitigation Program (CDM)

The Continuous Diagnostics and



GSA Cooperative Purchasing Program
With GSA's Cooperative Purchasing

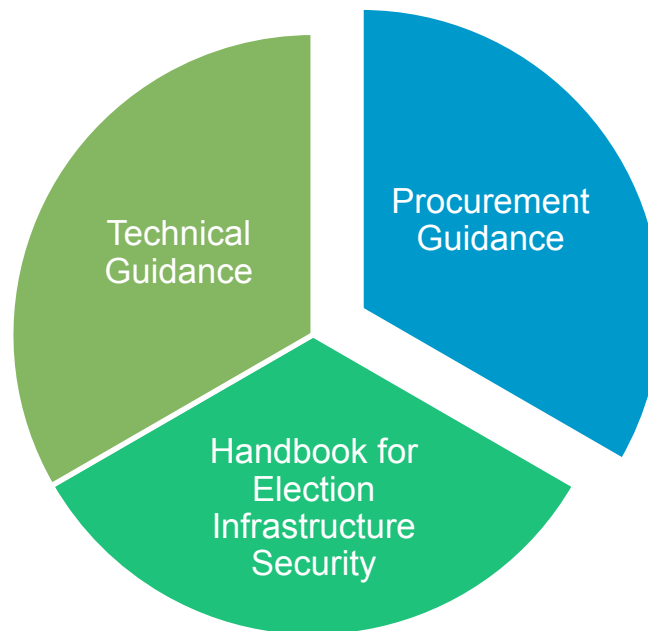


Third Party Breach Threat





Election Technology Procurements



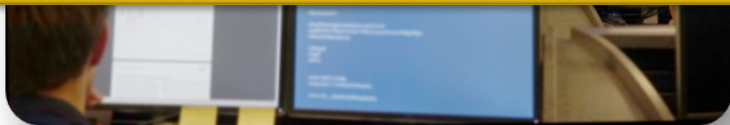


An Elections-focused Cyber Defense Suite

- 24x7x365 network monitoring
- Election-specific threat

If nothing else, know who you can contact and let us know who we should notify if we see anything.

When you hand me your contact information, let me know if you have special requests.



Join Us: learn.cisecurity.org/ei-isac-registration



MS-ISAC®

Multi-State Information
Sharing & Analysis Center®



**Elections
Infrastructure
ISAC**

EI-ISAC 24x7 Security Operations Center

1-866-787-4722

SOC@cisecurity.org

ELECTIONS@CISEcurity.ORG

Kateri Gill

Elections Program Manager

518.880.0779

Kateri.gill@cisecurity.org